QoS на установившихся контроллерах доступа и легковесном примере конфигурации AP

Содержание

Введение

Этот документ описывает, как настроить QoS в сходившемся доступе к сети Cisco с Облегченными точками доступа (LAP) и с Cisco Catalyst 3850 коммутаторов или Контроллер беспроводной локальной сети (WLC) Cisco 5760.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Базовые знания о том, как настроить LAP и Cisco, сходились контроллеры доступа
- Знание того, как настроить базовую маршрутизацию и QoS в проводной сети

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco Catalyst 3850 коммутаторов, которые выполняют Cisco IOS? Выпуск ПО XE 3.2.2 (SE)
- Контроллер беспроводной локальной сети Cisco 5760, который выполняет Выпуск 3.2.2 программного обеспечения Cisco IOS XE (SE)
- Точки доступа облегченных серий Cisco 3600

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

QoS обращается к способности сети предоставить улучшенное или особое обслуживание ряду пользователей или приложений в ущерб другим пользователям или приложений.

С QoS пропускной способностью можно управлять более эффективно через LAN, который включает беспроводные локальные сети (WLAN) и глобальные сети (WAN). QoS предоставляет улучшенному и надежному использованию сети эти сервисы:

- Выделенная полоса пропускания поддержек для важных пользователей и приложений.
- Управляет дрожанием и задержкой, которая требуется трафиком в реальном времени.
- Управляет и минимизирует перегрузку сети.
- Формирует сетевой трафик для сглаживания потока трафика.
- Приоритеты сетевого трафика наборов.

В прошлом WLAN в основном использовались для переноса низкой пропускной способности, трафика, связанного с данными приложений. С расширением WLAN в вертикальный (таких как розничная продажа, финансы и образование) и среды предприятия, WLAN теперь используются для переноса данных приложений, требующих высокой пропускной способности в сочетании с критичным по времени, мультимедийными приложениями. Это требование привело к необходимости беспроводного QoS.

Рабочая группа IEEE 802.11e в комитете по стандартам IEEE 802.11 завершила определение стандарта, и Wi-Fi Alliance создал Мультимедиа Wi-fi (WMM) сертификация, но все еще ограничено принятие 802.11e стандарт. Большинство устройств сертифицируется WMM, потому что сертификация WMM необходима для 802.11n и сертификация на 802.11 акра. Много беспроводных устройств не назначают другие уровни QoS на пакеты,

переданные к Канальному уровню, таким образом, те устройства передают большую часть своего трафика без маркировки QoS и никакой относительной приоритизации. Однако большинство IP-телефонов Системы голосовой связи на основе беспроводных локальных сетей (VoWLAN) 802.11 действительно отмечает и располагает по приоритетам свой голосовой трафик. Этот документ фокусируется на конфигурации QoS для IP-телефонов VoWLAN и на способных к видео устройствах Wi-fi, которые отмечают их голосовой трафик.

> **Примечание:** Конфигурация QoS для устройств, которые не выполняют внутреннюю маркировку, выходит за рамки этого документа.

802.11e поправка определяет восемь уровней приоритета пользователя (UP), сгруппированных два два в четыре уровня QoS (категории доступа):

- Платина/Голос (UP 7 и 6) - Гарантирует высокое качество сервиса для голоса по радио.
- Золото/Видео (UP 5 и 4) - Поддерживает высококачественные видеоприложения.
- Серебро/Оптимальный уровень (UP 3 и 0) - Поддерживает обычную пропускную способность для клиентов. Эта настройка используется по умолчанию.
- Бронза/Общие сведения (UP 2 и 1) - Предоставляет самую низкую пропускную способность для гостевых сервисов.

Платина обычно используется для клиентов VoIP и Золота для видео клиентов. Этот документ предоставляет пример конфигурации, который иллюстрирует, как настроить QoS на контроллерах и связаться с проводной сетью, которая настроена с QoS для VoWLAN и видео клиентов.

Усовершенствования маркировки пакетов QoS L3

Cisco сходилась маркировка Кодовой точки дифференцированных сервисов (DSCP) IP уровня поддержки 3 (L3) контроллеров доступа пакетов, переданных WLC и LAP. Эта функция улучшает, как точки доступа (AP) используют эту информацию о L3, чтобы гарантировать, что пакеты получают корректную беспроводную приоритизацию от AP до беспроводного клиента.

В установившейся архитектуре WLAN доступа, которая использует Коммутаторы Catalyst 3850 в качестве контроллеров беспроводной локальной сети, AP соединяются непосредственно с коммутатором. В установившейся архитектуре WLAN доступа, которая использует 5760 контроллеров, данные WLAN туннелированы между AP и WLC через Контроль и Инициализацию Точек беспроводного доступа (CAPWAP) протокол. Для поддержания исходной классификации QoS через этот туннель параметры настройки QoS инкапсулированного пакета данных должны быть соответственно сопоставлены с Уровнем 2 (L2) поля (802.1p) и L3 (IP DSCP) пакета внешнего туннеля.

При настройке QoS для VoWLAN и видео можно настроить политику QoS, определенную для беспроводных клиентов и политики, определенной для WLAN или обоих. Можно также дополнить настройку конфигурацией, определенной для порта, который связывает AP, особенно с Коммутаторами Catalyst 3850. Этот пример конфигурации фокусируется на конфигурации QoS для беспроводного клиента, WLAN и порта к AP. Основные задачи конфигурации QoS для VoWLAN и видеоприложений:

- Распознайте голос и видеотрафик (классификация трафика и отмечающий), оба

входящие и исходящие.
- Голос Марка и видеотрафик с уровнем приоритета голосовых данных: 802.11e UP 6, 802.1p 5, DSCP 46 для голоса.802.11e UP 5, DSCP 34 для видео.
- Выделите пропускную способность для голосового трафика, голосовой сигнализации и видеотрафика.

Настройте беспроводную сеть для QoS с MQC

Перед настройкой QoS необходимо настроить функцию Wireless Controller Module (WCM) Коммутатора Catalyst 3850 или WLC Cisco 5760 для главной операции и зарегистрировать LAP к WCM. Этот документ предполагает, что WCM настроен для главной операции и что LAP зарегистрированы к WCM.

Установившееся решение для доступа использует Модульный QoS (MQC) интерфейс командной строки (CLI). См. руководство по конфигурации конфигурации качества услуг QoS, Выпуск 3SE Cisco IOS XE (Коммутаторы Catalyst 3850) для дополнительных сведений об использовании MQC в конфигурации QoS на Коммутаторе Catalyst 3850.

Конфигурация QoS с MQC на установившихся контроллерах доступа полагается на четыре элемента:

- **Карты классов** используются для распознавания трафика интереса. Карты классов могут использовать различные способы (такие как существующая маркировка QoS, access-lists или VLAN) для определения трафика интереса.
- **Policy-map** используются для определения, какие параметры настройки QoS должны быть применены к трафику интереса. Policy-map вызывают карты классов и применяют различные параметры настройки QoS (такие как определенная маркировка, уровни приоритета, распределение пропускной способности, и так далее) к каждому классу.
- **Стратегии обслуживания** используются для применения policy-map к стратегическим точкам сети. В установившемся решении для доступа стратегии обслуживания могут быть применены к пользователям, Идентификаторы наборов сервисов (SSIDs), радио AP и порты. Порт, SSID и клиентская политика могут быть настроены пользователем. Радио-политика управляется беспроводным управляющим модулем. Когда трафик вытекает из коммутатора или контроллера беспроводным клиентам, беспроводные политики QoS для порта, SSID, клиента и радио применены в нижележащем направлении.
- **Table-map** используются для исследования входящей маркировки QoS и решить исходящие маркировки QoS. Table-map расположены в policy-map, применился к SSIDs. Table-map могут использоваться для хранения (копируют) или изменяют маркировку. Table-map могут также использоваться для создания сопоставления между проводной и беспроводной маркировкой. Проводная маркировка использует DSCP (QoS L3) или 802.1p (L2 QoS). Беспроводные сети, отмечающие Приоритет пользователя (UP) использования. Table-map обычно используются для определения, какая маркировка DSCP должна использоваться для каждого UP интереса и что UP должен использоваться для каждого DSCP-значения интереса. Table-map являются основным принципом установившегося QoS доступа, потому что нет никакой прямой трансляции между DSCP и значениями UP.

Однако DSCP к table-map UP также позволяет инструкцию *по копии*. В этом случае установившееся решение для доступа использует архитектуру Cisco для Голоса, Видео и

Итегрированных данных (AVVID) таблица соответствий для определения DSCP к UP или До трансляции DSCP:

Индекс метки	Ключевое поле	Входящее значение	Внешний DSCP	CoS	_____ включен
0	N.A.	Не проверенный	0	0	0
1-10	DSCP	0-7	0-7	0	0
11-18	DSCP	8-15	8-15	1	2
19-26	DSCP	16-23	16-23	2	3
27-34	DSCP	24-31	24-31	3	4
35-46	DSCP	32-39	32-39	4	5
47-48	DSCP	40-47	40-47	5	6
49-63	DSCP	48-55	48-55	6	7
64	DSCP	56-63	56-63	7	7
65	CoS	0	0	0	0
66	CoS	1	8	1	2
67	CoS	2	16	2	3
68	CoS	3	24	3	4
69	CoS	4	32	4	5
70	CoS	5	40	5	6
71	CoS	6	48	6	7
72	CoS	7	56	7	7
73	_____ включен	0	0	0	0
74	_____ включен	1	8	1	1
75	_____ включен	2	16	1	2
76	_____ включен	3	24	2	3
77	_____ включен	4	34	3	4
78	_____ включен	5	34	4	5
79	_____ включен	6	46	5	6
80	_____ включен	7	46	7	7

Жестко закодированная политика по умолчанию

Установившиеся контроллеры доступа загружают жестко закодированные профили политики QoS, которые могут быть применены к WLAN. Эти профили применяют металлическую политику (платина, золото, и так далее), которые знакомы администраторам контроллеров единых беспроводных сетей Cisco (UWN) (CUWN). Если ваша цель не состоит в том, чтобы создать политику, которая назначает определенную пропускную способность на голосовой трафик, но просто гарантировать, что голосовой трафик получает надлежащую маркировку QoS, можно использовать жестко закодированную политику. Жестко закодированная политика может быть применена к WLAN и может быть другой в восходящем и нижележащих направлениях.

Примечания:

Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show. Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

Платина

Жестко закодированную политику для голоса называют платиной. Название не может быть изменено.

Это - нисходящая политика для платинового уровня QoS:

```
Policy-map platinum
Class class-default
 set dscp dscp table plat-dscp2dscp
 set wlan user-priority dscp table plat-dscp2up
Table-map plat-dscp2dscp
   from 45 to 45
   from 46 to 46
   from 47 to 47
   default copy
Table-map plat-dscp2up
   from 34 to 4
   from 46 to 6
   default copy
```

Это - восходящая политика для Платинового уровня QoS:

```
Policy-map platinum-up
   Class class-default
     set dscp wlan user-priority table plat-up2dscp

Table-map plat-up2dscp
   from 4 to 34
   from 5 to 34
   from 6 to 46
   from 7 to 8
   default copy
```

Золото

Жестко закодированную политику для видео называют золотой. Название не может быть изменено.

Это - нисходящая политика для золотого уровня QoS:

```
Policy Map gold
   Class class-default
     set dscp dscp table gold-dscp2dscp
     set wlan user-priority dscp table gold-dscp2u
Table Map gold-dscp2dscp
   from 45 to 34
   from 46 to 34
```

```
   from 47 to 34
   default copy

Table Map gold-dscp2up
   from 45 to 4
   from 46 to 4
   from 47 to 4
   default copy
```

Это - восходящая политика для золотого уровня QoS:

```
Policy Map gold-up
   Class class-default
     set dscp wlan user-priority table gold-up2dscp

Table Map gold-up2dscp
   from 6 to 34
   from 7 to 34
   default copy
```

Серебро

Жестко закодированную политику для оптимального уровня называют серебряной. Название не может быть изменено.

Это - нисходящая политика для серебряного уровня QoS:

```
Policy Map silver
   Class class-default
     set dscp dscp table silver-dscp2dscp
     set wlan user-priority dscp table silver-dscp2up

Table Map silver-dscp2dscp
   from 34 to 0
   from 45 to 0
   from 46 to 0
   from 47 to 0
   default copy
Table Map silver-dscp2up
   from 34 to 0
  from 45 to 0
   from 46 to 0
   from 47 to 0
   default copy
```

Это - восходящая политика для серебряного уровня QoS:

```
Policy Map silver-up
   Class class-default
     set dscp wlan user-priority table silver-up2dscp
Table Map silver-up2dscp
   from 4 to 0
   from 5 to 0
   from 6 to 0
   from 7 to 0
   default copy
```

Бронза

Жестко закодированную политику для фонового трафика называют бронзовой. Название не может быть изменено.

Это - нисходящая политика для бронзового уровня QoS:

```
Policy Map bronze
   Class class-default
     set dscp dscp table bronze-dscp2dscp
 set wlan user-priority dscp table bronze-dscp2up

Table Map bronze-dscp2dscp
   from 0 to 8
   from 34 to 8
   from 45 to 8
   from 46 to 8
   from 47 to 8
   default copy

Table Map bronze-dscp2up
   from 0 to 1
   from 34 to 1
   from 45 to 1
   from 46 to 1
   from 47 to 1
   default copy
```

Это - восходящая политика для бронзового уровня QoS:

```
Policy Map bronze-up
   Class class-default
     set dscp wlan user-priority table bronze-up2dscp
Table Map bronze-up2dscp
   from 0 to 8
   from 1 to 8
   from 4 to 8
   from 5 to 8
   from 6 to 8
   from 7 to 8
   default copy
```

Как только вы решили, какой table-map лучше всего совпадает с целевым трафиком для данного SSID, можно применить соответствующую политику к WLAN. В данном примере одна политика применена в нижележащем направлении (выходные данные от AP до беспроводного клиента), и одна политика применена на восходящее направление (ввод, от беспроводного клиента, через AP, к контроллеру):

```
3850#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
3850(config)#wlan test1
3850(config-wlan)#service-policy output platinum
3850(config-wlan)#service-policy input platinum-up
3850(config-wlan)#end
3850#
```

Проверьте конфигурацию WLAN для проверки, какая политика была применена к WLAN:

```
3850#show wlan name test1
WLAN Profile Name    : test1
===============================================
Identifier                                 : 1
Network Name (SSID)                        : test1
Status                                     : Disabled
Broadcast SSID                             : Enabled
Maximum number of Associated Clients       : 0
AAA Policy Override                        : Disabled
Network Admission Control
 NAC-State                                : Disabled
```

```
Number of Active Clients                      : 0
Exclusionlist Timeout                         : 60
Session Timeout                               : 1800 seconds
CHD per WLAN                                  : Enabled
Webauth DHCP exclusion                        : Disabled
Interface                                     : default
Interface Status                              : Up
Multicast Interface                           : Unconfigured
WLAN IPv4 ACL                                 : unconfigured
WLAN IPv6 ACL                                 : unconfigured
DHCP Server                                   : Default
DHCP Address Assignment Required              : Disabled
DHCP Option 82                                : Disabled
DHCP Option 82 Format                         : ap-mac
DHCP Option 82 Ascii Mode                     : Disabled
DHCP Option 82 Rid Mode                       : Disabled
QoS Service Policy - Input
 Policy Name                                 : platinum-up
 Policy State                                : Validation Pending
QoS Service Policy - Output
 Policy Name                                 : platinum
 Policy State                                : Validation Pending
QoS Client Service Policy
 Input Policy Name                           : unknown
 Output Policy Name                          : unknown
WMM                                           : Allowed
Channel Scan Defer Priority:
 Priority (default)                          : 4
 Priority (default)                          : 5
 Priority (default)                          : 6
Scan Defer Time (msecs)                       : 100
Media Stream Multicast-direct                 : Disabled
CCX - AironetIe Support                       : Enabled
CCX - Gratuitous ProbeResponse (GPR)          : Disabled
CCX - Diagnostics Channel Capability          : Disabled
Dot11-Phone Mode (7920)                       : Invalid
Wired Protocol                                : None
Peer-to-Peer Blocking Action                  : Disabled
Radio Policy                                  : All
DTIM period for 802.11a radio                 : 1
DTIM period for 802.11b radio                 : 1
Local EAP Authentication                      : Disabled
Mac Filter Authorization list name            : Disabled
Accounting list name                          : Disabled
802.1x authentication list name               : Disabled
Security
   802.11 Authentication                      : Open System
   Static WEP Keys                            : Disabled
   802.1X                                     : Disabled
   Wi-Fi Protected Access (WPA/WPA2)          : Enabled
       WPA (SSN IE)                           : Disabled
       WPA2 (RSN IE)                          : Enabled
           TKIP Cipher                        : Disabled
           AES Cipher                         : Enabled
       Auth Key Management
           802.1x                             : Enabled
           PSK                                : Disabled
           CCKM                               : Disabled
   CKIP                                       : Disabled
   IP Security                                : Disabled
   IP Security Passthru                       : Disabled
   L2TP                                       : Disabled
   Web Based Authentication                   : Disabled
   Conditional Web Redirect                   : Disabled
```

```
   Splash-Page Web Redirect                  : Disabled
   Auto Anchor                               : Disabled
   Sticky Anchoring                          : Enabled
   Cranite Passthru                          : Disabled
   Fortress Passthru                         : Disabled
   PPTP                                      : Disabled
   Infrastructure MFP protection             : Enabled
   Client MFP                                : Optional
   Webauth On-mac-filter Failure             : Disabled
   Webauth Authentication List Name          : Disabled
   Webauth Parameter Map                     : Disabled
   Tkip MIC Countermeasure Hold-down Timer   : 60
Call Snooping                                 : Disabled
Passive Client                                : Disabled
Non Cisco WGB                                 : Disabled
Band Select                                   : Disabled
Load Balancing                                : Disabled
IP Source Guard                               : Disabled
```

Настройте вручную

Жестко закодированная политика применяет маркировку QoS по умолчанию, но не применяет распределение пропускной способности. Жестко закодированная политика также предполагает, что уже отмечен ваш трафик. В сложной среде можно хотеть использовать комбинацию политики, чтобы распознать и отметить голос и видеотрафик соответственно, чтобы установить распределение пропускной способности в нисходящем и восходящих направлениях, и использовать управление контролем доступа для ограничения количества Call Initiated от беспроводной ячейки.

> **Примечание:** Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Шаг 1: Идентификация и маркирование голосового трафика

Первый шаг должен распознать голос и видеотрафик. Голосовой трафик может быть классифицирован в две категории:

- Голосовой поток, который несет аудио часть связи.
- Голосовая сигнализация, которая несет статистическую информацию, которой обмениваются между речевыми оконечными точками.

Голосовой поток обычно использует порты назначения Протокола RTP и Протокола UDP в диапазоне 16384 - 32767. Это - диапазон; фактические порты являются обычно более узкими и зависят от реализации.

Существует несколько протоколов голосовой сигнализации. Этот пример конфигурации использует Jabber. Jabber использует эти порты TCP для соединения и каталога:

- (HTTP) TCP 80
- 143 (Интернет-сообщение протокол доступа [IMAP])
- 443 (HTTPS)
- 993 (IMAP) для сервисов, таких как Cisco Unified MeetingPlace или WebEx Cisco для совещаний и Cisco Unity или Cisco Unity Connection для функций голосовой почты

- TCP 389/636 (сервер Упрощенного протокола доступа к каталогам (LDAP) [LDAP] для поисков контакта)
- FTP (1080)
- TFTP (UDP 69) для передачи файла (такой как файлы конфигурации) от узлов или от сервера

Этим сервисам, возможно, не понадобится определенная приоритизация.

Jabber использует Протокол SIP (UDP/TCP 5060 и 5061) для голосовой сигнализации.

Видеотрафик использует другие порты и протоколы, которые зависят от вашей реализации. Этот пример конфигурации использует камеру Tandberg PrecisionHD 720 пунктов для видеоконференций. Камера Tandberg PrecisionHD 720 пунктов может использовать несколько кодеков; использованная пропускная способность зависит от выбранного кодека:

- C20, C40 и кодеки C60 используют H.323/SIP и могут использовать до 6 Мбит/с в двухточечных соединениях.
- Кодек C90 использует эти те же протоколы и может использовать до 10 Мбит/с в связи для нескольких местоположений.

Реализация Tandberg H.323, как правило, использует UDP 970 для потокового видео, UDP 971 для видео сигнализации, UDP 972 для потокового аудио и UDP 973 для аудио сигнализации. Камеры Tandberg также используют другие порты, такие как:

- UDP 161
- (Простой протокол управления сетью [SNMP]) UDP 962
- TCP 963 (netlog), (FTP) TCP 964
- (Virtual Network Computing [VNC]) TCP 965
- (Протокол объявления сеанса [SAP]) UDP 974

Этим дополнительным портам, возможно, не понадобится определенная приоритизация.

Обычный способ для определения трафика должен создать карты классов, которые предназначаются для трафика интереса. Каждый class-map может указать к access-list, который предназначается для любого трафика, который использует голос и видеопорты:

```
ip access-list extended JabberVOIP
permit udp any any range 16384 32767
ip access-list extended JabberSIGNALING
permit tcp any any range 5060 5061
permit udp any any range 5060 5061
ip access-list extended H323Videostream
permit udp any any eq 970
ip access-list extended H323Audiostream
permit udp any any eq 972
ip access-list extended H323VideoSignaling
permit udp any any eq 971
ip access-list extended H323AudioSignaling
permit udp any any eq 973
```

Можно тогда создать один class-map для каждого типа трафика; каждый class-map указывает к соответствующему access-list:

```
class-map RTPaudio
match access-group name JabberVOIP
match access-group name H323Audiostream
class-map H323realtimevideo
match access-group name H323Videostream
```

```
class-map signaling
match access-group name JabberSIGNALING
match access-group name H323VideoSignaling
match access-group name H323AudioSignaling
```

Как только голосовой трафик и видеотрафик были определены через карты классов, гарантируйте, что трафик отмечен должным образом. Это может быть сделано на уровне WLAN через table-map и может также быть сделано через клиентские policy-map.

Table-map исследуют маркировку QoS входящего трафика и определяют, какова исходящая маркировка QoS должна быть. Таким образом, когда входящий трафик уже имеет маркировку QoS, Table-map полезны. Table-map используются исключительно на уровне SSID.

В отличие от этого, policy-map могут предназначаться для трафика, определенного картами классов, и лучше адаптированы к потенциально немаркированному трафику интереса. Этот пример конфигурации предполагает, что трафик с проводной стороны был уже отмечен должным образом, прежде чем это введет Коммутатор Catalyst 3850 или WLC Cisco 5760. Если дело обстоит не так, можно использовать policy-map и применить его на уровне SSID как клиентская политика. Поскольку трафик от беспроводных клиентов не мог быть отмечен, необходимо отметить голос и видеотрафик должным образом:

- Оперативный голос должен быть отмечен (ускоренной пересылкой [EF]) DSCP 46.
- Видео должен быть отмеченный DSCP 34 (Уверенный Класс переадресации 41 [AF41]).
- Сигнализация для голоса и видео должна быть отмеченным DSCP 24 (Сервис селектора класса оценивают 3 [CS3]).

Для применения этих маркировок создайте policy-map, который вызывает каждый из этих классов, и это отмечает эквивалентный трафик:

```
policy-map taggingPolicy
 class RTPaudio
 set dscp ef

 class H323realtimevideo
 set dscp af41

 class signaling
 set dscp cs3
```

Шаг 2: Пропускная способность и приоритетный менеджмент на уровне порта

Следующий шаг должен определить политику QoS для портов, которые приходят и уходят к AP. Этот шаг прежде всего применяется к Коммутаторам Catalyst 3850. Если ваша конфигурация реализована на контроллере Cisco 5760, этот шаг не является обязательным. Catalyst 3850 портов несут голос и видеотрафик, который переходит или прибывает от беспроводных клиентов и AP. Конфигурация QoS в этом контексте совпадает с двумя требованиями:

1. **Выделите пропускную способность**. Можно хотеть решить, сколько пропускной способности выделено для каждого типа трафика. Это распределение пропускной способности может также быть сделано на уровне SSID. Приведите в порядок распределение пропускной способности порта для совершенствования, сколько пропускной способности может быть получено каждым AP, который служит целевому SSID. Эта пропускная способность должна быть установлена для всего SSIDs на

целевом AP. Этот пример упрощенной конфигурации предполагает, что существует только один SSID и один AP, таким образом, распределение пропускной способности порта для голоса и видео совпадает с глобальным распределением пропускной способности для голоса и видео на уровне SSID. Каждый тип трафика выделен 6 Мбит/с и охраняется так, чтобы не была превышена эта выделенная полоса.

2. **Расположите по приоритетам трафик**. Порт имеет четыре очереди. Первые две очереди расположены по приоритетам и зарезервированы для трафика реального времени - как правило, голос и видео, соответственно. Четвертая очередь зарезервирована для многоадресного трафика нев реальном времени, и третья очередь содержит весь другой трафик. С установившейся логикой организации очереди доступа трафик для каждого клиента назначен на действительную очередь, где может быть настроено QoS. Результат клиентской политики QoS введен в SSID действительная очередь, где может также быть настроено QoS. Так как несколько SSIDs могут существовать на данном радио AP, результат каждого SSID, который присутствует на радио AP, введен в радио AP действительная очередь, где трафик сформирован на основе радио-емкости. Трафик может быть задержан или отброшен на любом из этих этапов при помощи механизма QoS, названного Приблизительным справедливым отбрасыванием (AFD). Результат этой политики тогда передается порту AP (названный беспроводным портом), где приоритет отдан первым двум очередям (до конфигурируемой суммы пропускной способности), и затем третьим и четвертым очередям, как описано ранее в этом абзаце.

Этот пример конфигурации размещает голос в очередь основной задачи и видео в очереди с более низким приоритетом посредством использования команды **уровня приоритета**. Остаток трафика является выделенным остатком пропускной способности порта.

Заметьте, что вы не можете использовать карты классов, которые предназначаются для трафика на основе списков контроля доступа (ACL). Политика, примененная на уровне порта, может предназначаться для трафика на основе карт классов, но эти карты классов должны предназначаться для трафика, определенного его значением QoS. Как только вы имеете указанный трафик на основе ACL и отметили этот трафик должным образом на клиентском уровне SSID, это будет избыточно для выполнения второго глубокого контроля того же самого трафика на уровне порта. Когда трафик достигает порта, который переходит к AP, это уже отмечено должным образом.

В данном примере вы снова используете общие карты классов, созданные для политики SSID, и непосредственно предназначаетесь для речевого трафика RTP и видео трафика реального времени:

```
Class-map allvoice
match dscp ef
Class-map videoandsignaling
Match dscp af41
match dscp cs3
```

Как только вы определили трафик интереса, можно решить который политика примениться. Когда AP обнаружен, политика по умолчанию (названный parent_port) применена автоматически в каждом порту. Вы не должны изменять этот по умолчанию, который установлен как:

```
policy-map parent_port
class class-default
shape average 1000000000
```

```
service-policy port_child_policy
```

Поскольку по умолчанию parent_port политика вызывает port_child_policy, одна опция должна отредактировать port_child_policy. (Вы не должны менять его имя). Эта дочерняя политика определяет, какой трафик должен войти в каждую очередь и сколько пропускной способности должно быть выделено. У первой очереди есть наивысший приоритет, у второй очереди есть второй наивысший приоритет и так далее. Эти две очереди зарезервированы для трафика реального времени. Четвертая очередь используется для многоадресного трафика нев реальном времени. Третья очередь содержит весь другой трафик.

В данном примере вы решаете выделить голосовой трафик первой очереди и видеотрафик второй очереди и выделить пропускную способность каждой очереди и всему другому трафику:

```
Policy-map port_child_policy
Class allvoice
 Priority level 1
 police rate percent 10
 conform-action transmit
 exceed-action drop
class videoandsignaling
 priority level 2
 police rate percent 20
 conform-action transmit
 exceed-action drop
class non-client-nrt-class
 bandwidth remaining ratio 7
class class-default
 bandwidth remaining ratio 63
```

В этой политике приоритетное выражение, привязанное к 'голосу' и 'videoandsignaling' классам, позволяет вам назначать тот трафик на соответствующую очередь с приоритетами. Заметьте, однако, что операторы процента police rate применяются только для групповой адресации, не индивидуальная рассылка, трафик.

Вы не должны применять эту политику на уровне порта, потому что это применено автоматически, как только обнаружен AP.

Шаг 3: Пропускная способность и приоритетный менеджмент на уровне SSID

Следующий шаг должен заботиться о политике QoS на уровне SSID. Этот шаг применяется к и Коммутатору Catalyst 3850 и к 5760 контроллерам. Эта конфигурация предполагает, что голос и видеотрафик определены с помощью class-map и access-lists и помечены должным образом. Однако некоторый входящий трафик, который не предназначен access-list, может не отобразить свою маркировку QoS. В этом случае можно решить, должен ли этот трафик быть отмечен значением по умолчанию или оставлен без меток. Та же логика идет для трафика, уже отмеченного, но не предназначенная картами классов. Используйте оператор *стандартной копии* в table-map, чтобы гарантировать, что неотмеченный трафик оставляют не отмеченным и что помеченный трафик поддерживает метку и это не отмеченными.

Table-map решают исходящее DSCP-значение, но также используются для создания кадра 802.11 для решения значения UP кадра.

В данном примере входящий трафик, который отображает речевой уровень QoS (DSCP 46), поддерживает свое DSCP-значение, и значение сопоставлено с эквивалентной маркировкой 802.11 (UP 6). Входящий трафик, который отображает видео уровень QoS (DSCP 34),

поддерживает свое DSCP-значение, и значение сопоставлено с эквивалентной маркировкой 802.11 (UP 5). Точно так же отмеченный DSCP 24 трафика может быть голосовой сигнализацией; DSCP-значение должно быть поддержано и преобразовано в 802.11 UP 3:

```
Table-map dscp2dscp
Default copy
Table-map dscp2up
Map from 46 to 6
Map from 24 to 3
Map from 34 to 5
Default copy
```

Маркирование могло также быть сделано на соединенном проводом уровне порта поступления. Эти данные показывают, какие действия QoS могут быть взяты в качестве транзитов трафика от проводного до радио:

Этот пример конфигурации фокусируется на беспроводном аспекте конфигурации QoS и трафика меток на уровне беспроводного клиента. Как только часть маркировки была завершена, необходимо выделить пропускную способность; здесь, 6 Мбит/с пропускной способности выделены потокам голосового трафика. (В то время как это - выделение суммарной пропускной способности для голоса, каждый вызов использовал бы менее - например, 128 кбит/с.) Эта пропускная способность выделена с командой **политики** для резервирования пропускной способности и отбрасывать трафик в избытке.

Видеотрафик также выделяется 6 Мбит/с и охраняется. Этот пример конфигурации предполагает, что существует только один видео поток.

Сигнальная часть видео и голосового трафика также должна быть выделенной полосой. Существует две возможных стратегии.

- Используйте **команду shape average**, которая позволяет трафику в избытке быть буферизованным и переданным позже. Эта логика не эффективна для голоса или самого видео потока, потому что те потоки требуют последовательной задержки и дрожания; однако, это может быть эффективно для сигнализации, потому что сигнализация может быть немного задержана без эффекта на качество вызова. В установившемся решении для доступа команды формы не принимают то, что называют "конфигурациями блоков", которые определяют, сколько трафика сверх выделенной полосы может быть буферизовано. Поэтому вторая команда, **соотношение буферов очереди 0**, должна быть добавлена, чтобы указать, что размер блока 0. Если вы включаете сигнализацию в остаток трафика и используете команды формы, трафик сигнализации мог бы быть отброшен во времена высокого уровня перегрузки. Этот мог бы, в свою очередь, заставить вызов быть отброшенным, потому что любой конец решает, что больше не происходит связь.
- Для предотвращения риска разрывов связи можно включать сигнализацию в одну из очередей с приоритетами. Этот пример конфигурации ранее определил очереди с приоритетами как голос и видео и теперь добавляет сигнализацию к видео-очереди.

Политика использует управление контролем доступа (CAC) для голосового потока. CAC предназначается для беспроводного трафика и подходит определенное (в этом примере конфигурации, UP 6 и 7). CAC тогда определяет максимальную пропускную способность, которую должен использовать этот трафик. В конфигурации, где вы определяете политику голосового трафика, CAC должен быть выделен подмножество полной суммы пропускной способности, выделенной для голоса. Например, если голос охраняется к 6 Мбит/с, CAC не может превысить 6 Мбит/с. CAC настроен в policy-map (названный дочерней политикой),

который интегрирован в основной нисходящий policy-map (названный родительской политикой). CAC представлен с **допущением cac wmm-tspec** команда, придерживавшаяся к установленному сроку UPs и пропускная способность, выделенная предназначенному трафику.

Каждый вызов не использует всю пропускную способность, выделенную голосу. Например, каждый вызов может использовать 64 кбит/с каждый путь, который приводит к 128 кбит/с эффективной двунаправленной потребляемой полосы пропускания. В то время как инструкция политики определяет суммарную пропускную способность, выделенную голосовому трафику, инструкция по скорости определяет каждое потребление трафика при вызове. Если все вызовы, которые происходят в рамках использования ячейки близко к максимальну допустимому ширина полосы пропускания, какой-либо новый вызов, который инициируется из ячейки и это заставляет использованную пропускную способность превышать максимальную пропускную способность, обеспечил голос, будет запрещен. Можно точно настроить этот процесс через конфигурацию CAC на уровне полосы, как объяснено в Шаге 4: Ограничение вызовов с CAC.

Поэтому необходимо настроить дочернюю политику, которая содержит инструкции по CAC, и это интегрировано в основную нисходящую политику. CAC не настроен в восходящем policy-map. CAC действительно применяется к голосовым вызовам, инициируемым от ячейки, но, потому что это - ответ на те вызовы, CAC установлен только в нисходящий policy-map. Восходящий policy-map будет другим. Вы не можете использовать карты классов, созданные ранее, потому что эти карты классов предназначаются для трафика на основе ACL. Трафик, введенный в политику SSID уже, прошел клиентскую политику, таким образом, вы не должны выполнять глубокий контроль на пакетах во второй раз. Вместо этого целевой трафик с QoS, отмечающим, который следует из клиентской политики.

Если вы решите не оставить сигнализацию в классе по умолчанию, то необходимо будет также расположить по приоритетам сигнализацию.

В данном примере, сигнализируя и видео находятся в том же классе, и больше пропускной способности выделено тому классу для размещения сигнальной части; 6 Мбит/с выделены для видеотрафика (один поток точка-точка камеры Tandberg), и 1 Мбит/с выделен сигнализации для всех голосовых вызовов и видео потока:

```
Class-map allvoice
match dscp ef
Class-map videoandsignaling
Match dscp af41
Match dscp cs3
```

Нисходящая дочерняя политика:

```
Policy-map SSIDout_child_policy
class allvoice
priority level 1
police 6000000
admit cac wmm-tspec
rate 128
wlan-up 6 7
class videoandsignaling
priority level 2
police 1000000
```

Нисходящая родительская политика:

```
policy-map SSIDout
class class-default
```

```
set dscp dscp table dscp2dscp
set wlan user-priority dscp table dscp2up
shape average 30000000
queue-buffers ratio 0
service-policy SSIDout_child_policy
```

Трафик восходящего направления является трафиком, который прибывает от беспроводных клиентов и передается WCM, прежде чем трафик будет передан из проводного порта или будет передан другому SSID. В обоих случаях можно настроить policy-map, которые определяют пропускную способность, выделенную каждому типу трафика. Политика будет, вероятно, отличаться на основе того, передается ли трафик из проводного порта или к другому SSID.

В восходящем направлении ваше основное предприятие должно решить приоритет, не пропускную способность. Другими словами, ваш восходящий policy-map не выделяет пропускную способность каждому типу трафика. Поскольку трафик уже в AP и уже пересек узкое место, сформированное полудуплексным беспроводным пространством, ваша цель состоит в том, чтобы принести этот трафик к функции контроллера Коммутатора Catalyst 3850 или WLC Cisco 5760 для дальнейшей обработки. Когда трафик собран на уровне AP, можно решить, необходимо ли доверять потенциальной существующей маркировке QoS для расположения по приоритетам трафиков, передаваемых контроллеру. В данном примере можно доверять существующим DSCP-значениям:

```
Policy-map SSIDin
Class class-default
set dscp dscp table dscp2dscp
```

Как только ваша политика создана, применяет policy-map к WLAN. В данном примере любое устройство, которое соединяется с WLAN, как ожидают, поддержит WMM, таким образом, будет требоваться WMM.

```
wlan test1
wmm require
service-policy client input taggingPolicy
service-policy input SSIDin
service-policy output SSIDout
```

Шаг 4. : Ограничение вызовов с CAC

Последний шаг должен адаптировать CAC в соответствии с вашей определенной ситуацией. В конфигурации CAC, объясненной в Шаге 3: Пропускная способность и Приоритетный менеджмент на Уровне SSID, AP отбрасывает любой голосовой пакет, который превышает выделенную полосу.

Во избежание максимума пропускной способности., также необходимо настроить WCM для распознавания вызовов, которые размещены и вызовы, которые заставят пропускную способность быть превышенной. Некоторые телефоны поддерживают Спецификацию Трафика WMM (TSPEC) и сообщают беспроводной инфраструктуре пропускной способности, что спроектированный вызов, как ожидают, использует. WCM может тогда отказаться от вызова, прежде чем это будет размещено.

Некоторые SIP-телефоны не поддерживают TSPEC, но WCM и AP могут собираться распознать пакеты инициации вызова, переданные портам SIP, и могут использовать эту информацию, чтобы установить, что вызов SIP собирается быть размещенным. Поскольку SIP-телефон не задает пропускную способность, которая должна быть использована вызовом, администратор должен определить ожидаемую пропускную способность, на

основе кодека, интервал дискретизации, и так далее.

CAC вычисляет использованную пропускную способность на каждом уровне AP. CAC может собираться использовать только клиентскую потребляемую полосу пропускания в своих вычислениях (статический CAC) или также рассмотреть соседние AP и устройства на том же канале (основанный на загрузке CAC). Cisco рекомендует использовать статический CAC для SIP-телефонов и основанный на загрузке CAC для телефонов TSPEC.

Наконец, обратите внимание, что CAC активирован на на основание полосы.

В данном примере, SIP использования телефонов, а не TSPEC для их инициирования сеанса, каждый вызов использует 64 кбит/с для каждого направления потока, основанный на загрузке CAC отключен, когда статический CAC включен, и 75% каждой пропускной способности AP макс. выделены голосовому трафику:

```
ap dot11 5ghz shutdown
ap dot11 5ghz cac voice acm
no ap dot11 5ghz cac voice load-based
ap dot11 5ghz cac voice max-bandwidth 75
ap dot11 5ghz cac voice sip bandwidth 64
no ap dot11 5ghz shutdown
```

Можно повторить одинаковую конфигурацию для полосы на 2.4 ГГц:

```
ap dot11 24ghz shutdown
ap dot11 24ghz cac voice acm
no ap dot11 24ghz cac voice load-based
ap dot11 24ghz cac voice max-bandwidth 75
ap dot11 24ghz cac voice sip bandwidth 64
no ap dot11 24ghz shutdown
```

Как только CAC применен для каждой полосы, также необходимо применить CAC SIP на уровне WLAN. Этот процесс позволяет AP исследовать Уровень 4 (L4) информация трафика беспроводного клиента для определения запросов, передаваемых UDP 5060, которые указывают на попытки вызова SIP. TSPEC работает на уровне 802.11 и исходно обнаружен AP. SIP-телефоны не используют TSPEC, таким образом, AP должен выполнить более глубокую проверку пакетов для определения трафика SIP. Поскольку вы не хотите, чтобы AP выполнил этот контроль на всем SSIDs, необходимо определить, какие SSIDs ожидают трафик SIP. Можно тогда включить вызов, snooping на тех SSIDs для поиска голосовых вызовов. Можно также определить, какое действие выполнить, если вызов SIP должен быть отклонен - разъединяют клиента SIP или передают сообщению о загруженности SIP.

В данном примере звоните, отслеживание включено, и сообщение о загруженности передается, если должен быть отклонен вызов SIP. С добавлением политики QoS от Шага 3: Пропускная способность и Приоритетный менеджмент на Уровне SSID, это - конфигурация SSID для WLAN в качестве примера:

```
wlan test1
wmm require
service-policy client input taggingPolicy
service-policy input SSIDin
service-policy output SSIDout
call-snoop
sip-cac send-486busy
```

Проверка

Используйте эти команды, чтобы подтвердить, что ваша конфигурация QoS работает должным образом.

> **Примечания:**
>
> Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).
>
> Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

show class-map

Эта команда отображает карты классов, настроенные на платформе:

```
3850#show class-map
 Class Map match-any H323realtimeaudio (id 6)
  Match access-group name H323Audiostream
Class Map match-any H323realtimevideo (id 7)
  Match access-group name H323Videostream
Class Map match-any allvideo (id 10)
  Match  dscp af41 (34)
Class Map match-any jabberaudiosignaling (id 11)
  Match access-group name JabberSIGNALING
Class Map match-any allvoice (id 12)
  Match  dscp ef (46)
Class Map match-any RTPaudio (id 19)
  Match access-group name JabberVOIP
  Match access-group name H323Audiostream
Class Map match-any class-default (id 0)
  Match any
Class Map match-any jabberRTPaudio (id 14)
  Match access-group name JabberVOIP
Class Map match-any non-client-nrt-class (id 1)
  Match non-client-nrt
Class Map match-any H323audiosignaling (id 17)
  Match access-group name H323AudioSignaling
Class Map match-any H323videosignaling (id 18)
  Match access-group name H323VideoSignaling
Class Map match-any signaling (id 20)
  Match access-group name JabberSIGNALING
  Match access-group name H323VideoSignaling
  Match access-group name H323AudioSignaling
```

show policy-map

Эта команда отображает policy-map, настроенные на платформе:

```
3850 #show policy-map
show policy-map
 Policy Map port_child_policy
   Class non-client-nrt-class
     bandwidth remaining ratio 7
   Class allvoice
     priority level 1
```

```
    police rate percent 10
      conform-action transmit
      exceed-action drop
   Class allvideo
     priority level 2
    police rate percent 20
      conform-action transmit
      exceed-action drop
   Class class-default
     bandwidth remaining ratio 63
 Policy Map SSIDin
   Class class-default
     set dscp dscp table dscp2dscp
 Policy Map SSIDout_child_policy
   Class allvoice
     priority level 1
    police cir 6000000 bc 187500
      conform-action transmit
      exceed-action drop
     admit cac wmm-tspec
       rate 6000 (kbps)
       wlan-up 6
   Class allvideo
     priority level 2
    police cir 6000000 bc 187500
      conform-action transmit
      exceed-action drop
     admit cac wmm-tspec
       rate 6000 (kbps)
       wlan-up 4 5
 Policy Map taggingPolicy
   Class RTPaudio
     set dscp ef
   Class H323realtimevideo
     set dscp af41
   Class signaling
     set dscp cs3
 Policy Map SSIDout
   Class class-default
     set dscp dscp table dscp2dscp
     set wlan user-priority dscp table dscp2up
     shape average 30000000 (bits/sec)
     queue-buffers ratio 0
     service-policy SSIDout_child_policy
 Policy Map parent_port
   Class class-default
     shape average 1000000000 (bits/sec) op
```

show wlan

Эта команда отображает параметры стратегии обслуживания и конфигурация WLAN:

```
3850# show wlan name test1 | include Policy
AAA Policy Override                          : Disabled
QoS Service Policy - Input
 Policy Name                                 : SSIDin
 Policy State                                : Validated
QoS Service Policy - Output
 Policy Name                                 : SSIDout
 Policy State                                : Validated
QoS Client Service Policy
 Input Policy Name                          : taggingPolicy
```

```
 Output Policy Name                          : taggingPolicy
Radio Policy                                  : All
```

show policy-map interface

Эта команда отображает policy-map, установленный для определенного интерфейса:

```
3850#show policy-map interface wireless ssid name test1

Remote SSID test1 iifid: 0x01023F4000000033.0x00F2E98000000003.0x00C2EB000000001F
 Service-policy input: SSIDin
   Class-map: class-default (match-any)
     Match: any
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp dscp table dscp2dscp

Remote SSID test1 iifid: 0x01023F4000000033.0x00C8384000000004.0x00D0D08000000021

 Service-policy input: SSIDin

   Class-map: class-default (match-any)
     Match: any
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp dscp table dscp2dscp

SSID test1 iifid: 0x01023F4000000033.0x00F2E98000000003.0x00EC3E800000001E

 Service-policy input: SSIDin

   Class-map: class-default (match-any)
     Match: any
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp dscp table dscp2dscp

 Service-policy output: SSIDout

   Class-map: class-default (match-any)
     Match: any
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp dscp table dscp2dscp
       wlan user-priority dscp table dscp2up
     shape (average) cir 30000000, bc 120000, be 120000
     target shape rate 30000000
     queue-buffers ratio 0

     Service-policy : SSIDout_child_policy

       Class-map: allvoice (match-any)
         Match: dscp ef (46)
           0 packets, 0 bytes
           30 second rate 0 bps
         Priority: Strict,

         Priority Level: 1
```

```
        police:
            cir 6000000 bps, bc 187500 bytes
          conformed 0 bytes; actions:
            transmit
          exceeded 0 bytes; actions:
            drop
          conformed 0000 bps, exceed 0000 bps
        cac wmm-tspec rate 6000 kbps

      Class-map: allvideo (match-any)
        Match: dscp af41 (34)
          0 packets, 0 bytes
          30 second rate 0 bps
        Priority: Strict,

        Priority Level: 2
        police:
            cir 6000000 bps, bc 187500 bytes
          conformed 0 bytes; actions:
            transmit
          exceeded 0 bytes; actions:
            drop
          conformed 0000 bps, exceed 0000 bps
        cac wmm-tspec rate 6000 kbps

      Class-map: class-default (match-any)
        Match: any
          0 packets, 0 bytes
          30 second rate 0 bps

SSID test1 iifid: 0x01023F4000000033.0x00C8384000000004.0x00DB568000000020

 Service-policy input: SSIDin

   Class-map: class-default (match-any)
     Match: any
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp dscp table dscp2dscp

 Service-policy output: SSIDout

   Class-map: class-default (match-any)
     Match: any
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp dscp table dscp2dscp
       wlan user-priority dscp table dscp2up
     shape (average) cir 30000000, bc 120000, be 120000
     target shape rate 30000000
     queue-buffers ratio 0

     Service-policy : SSIDout_child_policy

       Class-map: allvoice (match-any)
         Match: dscp ef (46)
           0 packets, 0 bytes
           30 second rate 0 bps
         Priority: Strict,

         Priority Level: 1
         police:
```

```
            cir 6000000 bps, bc 187500 bytes
          conformed 0 bytes; actions:
            transmit
          exceeded 0 bytes; actions:
            drop
          conformed 0000 bps, exceed 0000 bps
        cac wmm-tspec rate 6000 kbps

      Class-map: allvideo (match-any)
        Match: dscp af41 (34)
          0 packets, 0 bytes
          30 second rate 0 bps
        Priority: Strict,

        Priority Level: 2
        police:
            cir 6000000 bps, bc 187500 bytes
          conformed 0 bytes; actions:
            transmit
          exceeded 0 bytes; actions:
            drop
          conformed 0000 bps, exceed 0000 bps
        cac wmm-tspec rate 6000 kbps

      Class-map: class-default (match-any)
        Match: any
          0 packets, 0 bytes
          30 second rate 0 bps

3850#show policy-map interface wireless client
Client 8853.2EDC.68EC iifid:
0x01023F4000000033.0x00F2E98000000003.0x00EC3E800000001E.0x00E0D04000000022

 Service-policy input: taggingPolicy

   Class-map: RTPaudio (match-any)
     Match: access-group name JabberVOIP
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: access-group name H323Audiostream
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp ef

   Class-map: H323realtimevideo (match-any)
     Match: access-group name H323Videostream
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp af41

   Class-map: signaling (match-any)
     Match: access-group name JabberSIGNALING
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: access-group name H323VideoSignaling
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: access-group name H323AudioSignaling
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp cs3
```

```
   Class-map: class-default (match-any)
     Match: any
       0 packets, 0 bytes
       30 second rate 0 bps

 Service-policy output: taggingPolicy

   Class-map: RTPaudio (match-any)
     Match: access-group name JabberVOIP
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: access-group name H323Audiostream
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp ef

   Class-map: H323realtimevideo (match-any)
     Match: access-group name H323Videostream
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp af41

   Class-map: signaling (match-any)
     Match: access-group name JabberSIGNALING
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: access-group name H323VideoSignaling
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: access-group name H323AudioSignaling
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp cs3
   Class-map: class-default (match-any)
     Match: any
       0 packets, 0 bytes
       30 second rate 0 bps
```

политика show platform qos

Эта команда отображает политики QoS, установленные для портов, радио AP, SSIDs и клиентов. Заметьте, что вы можете проверить, но не можете измениться, радио-политика:

```
3850#show platform qos policies PORT
Loc Interface         IIF-ID            Dir Policy          State
--- ------------------ ------------------ --- --------------- ---------------
L:0 Gi1/0/20          0x01023f4000000033 OUT defportangn     INSTALLED IN HW
L:0 Gi1/0/20          0x01023f4000000033 OUT port_child_policyINSTALLED IN HW

3850#show platform qos policies RADIO
Loc Interface         IIF-ID            Dir Policy          State
--- ------------------ ------------------ --- --------------------------------
L:0 R56356842871193604 0x00c8384000000004 OUT def-11an        INSTALLED IN HW
L:0 R68373680329064451 0x00f2e98000000003 OUT def-11gn        INSTALLED IN HW
3850#show platform qos policies SSID
Loc Interface         IIF-ID            Dir Policy          State
--- ------------------ ------------------ --- --------------------------------
L:0 S70706569125298203 0x00fb33400000001b OUT SSIDout_child_policyINSTALLED IN HW
L:0 S69318160817324057 0x00f6448000000019 OUT SSIDout_child_policyINSTALLED IN HW
```

```
L:0 S70706569125298203 0x00fb33400000001b OUT SSIDout         INSTALLED IN HW
L:0 S69318160817324057 0x00f6448000000019 OUT SSIDout         INSTALLED IN HW
L:0 S70706569125298203 0x00fb33400000001b IN SSIDin          INSTALLED IN HW
L:0 S69318160817324057 0x00f6448000000019 IN SSIDin          INSTALLED IN HW

3850#show platform qos policies CLIENT
Loc Interface         IIF-ID            Dir Policy          State
--- ----------------- ----------------- --- --------------- --------------
L:0 8853.2edc.68ec    0x00e0d04000000022 IN taggingPolicy   NOT INSTALLED IN HW
L:0 8853.2edc.68ec    0x00e0d04000000022 OUT taggingPolicy   NOT INSTALLED IN HW
```

покажите mac-address беспроводного клиента <Mac> стратегия обслуживания

Эта команда отображает policy-map, примененные на клиентском уровне:

```
3850#show wireless client mac-address 8853.2EDC.68EC service-policy output
Wireless Client QoS Service Policy
Policy Name : taggingPolicy
Policy State : Installed
3850#sh wireless client mac-address 8853.2EDC.68EC service-policy in
3850#sh wireless client mac-address 8853.2EDC.68EC service-policy input
Wireless Client QoS Service Policy
Policy Name : taggingPolicy
Policy State : Installed
```

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.